United States Naval Academy

Access and Use

of

Information Technology Resources

Superintendent's Executive Board

January 1998

Information Technology Resources Definition

- **All computing systems**
  - devices which contain a processing unit
  - devices which can be connected to the processing unit
  - all software
  - all hardware
- **All communications systems**
  - Data communications
  - Voice communications
  - Video communications
  - devices (telephones, facsimile machines, cellular phones, pagers, copiers, messaging systems, internet systems

Use of Information Technology

- Official
  - Directly execute the USNA mission

- Authorized
  - Supports the mission be ensuring a productive work environment.

Authorized Use

- Determined by appropriate supervisor

- First supervisor, a commissioned officer, a civilian faculty, or a civilian above the GS - 11

Authorized Use - Personal use

- Includes personal communications from the employee's workplace when permitted by the appropriate supervisor as long as:
  - Does not adversely affect employee's performance of duties
  - Is of reasonable duration and frequency
  - Whenever possible made during individual's personal time
  - Serves a legitimate public interest - keep individual at their desk, improve morale, enhance professional skills, further education
  - Does not reflect adversely on USNA
  - Does not overburden or adversely impact performance of resources
  - Does not create additional cost to USNA

Guidelines

- Use information technology resources for authorized education, research, and administrative activities in support of the Naval Academy mission.

- Any document, object, or file containing privacy data or information will be properly safeguarded to prevent unauthorized access and use. Appropriate protective measures will be taken to protect and backup information and applications.

- Users will not access or attempt to access unauthorized systems, files, and information.

Guidelines

- Users will protect their individual accounts and passwords. Users will not provide their account and/or password to other individuals. Passwords will be changed every four months.

- Resources cannot be used for illegal purposes (unauthorized copying or use of copyrighted material; possessing, copying or using illegal software; destruction or damage to Naval Academy or personal resources; disruption or unauthorized monitoring of communications; or harassment of other users).

- Users will not introduce or use malicious software, computer viruses, Trojan horses, or computer worms. Users will report suspected occurrences of viruses or any suspicious activity to their system administrator.

Guidelines

- Users will be aware of the licensing terms and conditions for all software on their computing resources or accessed via the networks.

- Users will not create, save, send, receive, or access inappropriate material (which includes, but not limited to, pornography, threats, racist, vulgarity, malicious, obscenity, or sexual explicit)

- Use information technology resources in accordance with ethical standards. Examples of unethical use, which may also be illegal, include:

Guidelines

- Dishonesty (plagiarism, cheating)
- Violation of another individual's privacy
- Violation of license agreements
- Violation of network usage
- Intentional use of resources which impede the activities of others
- Unauthorized use of accounts, access codes, and passwords
- Unauthorized access or use of data and files
- Violations of system security

Authorized Users

- Midshipmen
- Faculty
- Staff
- Tenants
- Reimbursable Accounts
- Non-Appropriated Fund Activities

User's Responsibility

- By using or accessing Naval Academy information technology resources, each user automatically assumes the responsibility for using this information technology resource within legal and ethical boundaries.

- Access to most computer systems and computer programs require user accounts and passwords.

- Personnel are only issued accounts and passwords for themselves and may not be shared.

Privacy and Monitoring

- Information technology resources are inherently insecure. These resources are not private. Use of these resources consent to monitoring of the resource. Information technology resources may be monitored for all lawful purposes, including to ensure authorized use, for management of the resources, to ensure operational performance, to facilitate protection against unauthorized access, and to verify security procedures and operational security.

Monitoring

afdahl.infotech.nadn.navy.mil

----

   altavista.digital.com   204.123.2.69   1/14/1998

   dhcp155-11.dhcp.nadn.navy.mil   131.121.155.11   1/14/1998

Disciplinary Actions

- Civilian   Reprimand to removal
- Midshipman
- Military